

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-333407

(43)Date of publication of application : 30.11.2001

(51)Int.Cl. H04N 7/167
 H04H 1/00
 H04L 9/08
 H04L 9/10
 H04N 5/44
 H04N 5/76
 H04N 5/91
 H04N 7/08
 H04N 7/081
 // H04N 7/20

(21)Application number : 2000-153438

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 24.05.2000

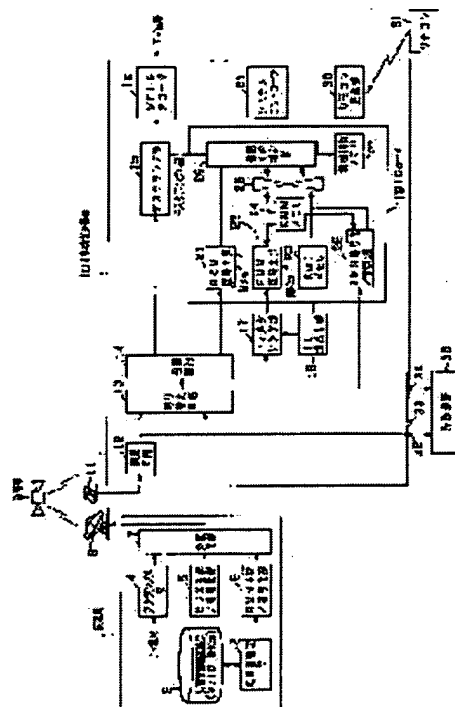
(72)Inventor : OI SHINICHI

(54) PAY BROADCAST SYSTEM, PAY BROADCAST RECEIVER AND PAY BROADCAST TIME SHIFT VIEWING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a pay broadcast system that can prevent illegal viewing in time shift viewing.

SOLUTION: An EMM generating/encryption section 6 of a broadcast station 1 generates an EMM(entitlement management message) that includes information not only at the end of a view contract but also at the start thereof. In the case of time-shift viewing, a view propriety decision section 26 receives the EMM reproduced from a recorder 35. The view propriety decision section 26 uses the information at the start and end of a view contract included in the EMM for the decision of view propriety. Thus, even when the EMM reproduced from the recorder 35 is not compatible with program data and no view contract is made at the broadcast of a reproduced program, the system can prevent illegal viewing.



LEGAL STATUS

[Date of request for examination]

18.02.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-333407

(P2001-333407A)

(43) 公開日 平成13年11月30日 (2001.11.30)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
H 0 4 N	7/167	H 0 4 H 1/00	F 5 C 0 2 5
H 0 4 H	1/00	H 0 4 N 5/44	A 5 C 0 5 2
H 0 4 L	9/08		Z 5 C 0 5 3
	9/10	5/76	Z 5 C 0 6 3
H 0 4 N	5/44	7/20	6 3 0 5 C 0 6 4

審査請求 未請求 請求項の数 6 O L (全 13 頁) 最終頁に続く

(21) 出願番号 特願2000-153438(P2000-153438)

(22) 出願日 平成12年5月24日(2000.5.24)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 大井 伸一

神奈川県横浜市磯子区新杉田町8番地 株式会社東芝横浜事業所内

(74) 代理人 100076233

弁理士 伊藤 進

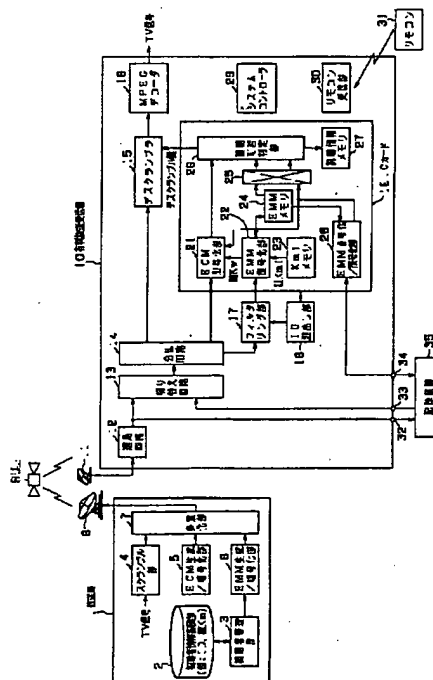
最終頁に続く

(54) 【発明の名称】 有料放送システム、有料放送受信機及び有料放送タイムシフト視聴方法

(57) 【要約】

【課題】 タイムシフト視聴時における不正視聴を防止する。

【解決手段】 放送局1のEMM生成/暗号化部6は、視聴契約の終了時だけでなく、開始時の情報を含むEMMを生成する。タイムシフト視聴時には記録装置35から再生されたEMMが視聴可否判定部26に供給される。視聴可否判定部26は、視聴可否の判定に際して、EMMに含まれる視聴契約の開始及び終了時の情報を用いる。これにより、記録装置35から再生されるEMMと番組データとが対応しない場合であって、再生番組の放送時に視聴契約が行われていない場合であっても、不正視聴を防止することができる。



【特許請求の範囲】

【請求項1】 番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報を暗号化するために用いられるワーク鍵と、視聴契約の内容に応じた情報と、を含む個別情報であって、前記視聴契約の開始及び終了時の情報を含む個別情報を生成する個別情報生成手段を具備したことを特徴とする有料放送システム。

【請求項2】 番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信手段と、前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する視聴可否判定手段とを具備したことを特徴とする有料放送受信機。

【請求項3】 番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する受信手段と、前記受信手段が受信した個別情報を取得する個別情報取得手段と、前記個別情報取得手段が取得した前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手段と、前記個別情報取得手段が取得した個別情報と前記番組情報取得手段が取得した番組情報とを組にして暗号化して出力する暗号化手段と、前記受信手段が受信した番組データ及び前記暗号化手段からの暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手段と、前記番組情報と前記個別情報とに基づいて、番組データの視聴の可否を判定するものであって、前記記録手段が再生した番組データに含まれる番組情報を前記番組情報取得手段が前記復号化手段からの個別情報中のワーク鍵を用いて復号化して得た番組情報と前記復号化手段からの番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手段とを具備したことを特徴とする有料放送受信機。

【請求項4】 前記個別情報取得手段、前記番組情報取得手段、前記暗号化手段、前記復号化手段及び前記視聴可否判定手段は、集積回路化されていることを特徴とする請求項3に記載の有料放送受信機。

【請求項5】 番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信手段と、

前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する手段とを具備したことを特徴とする有料放送タイムシフト視聴方法。

【請求項6】 番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する手段と、

受信した個別情報を取得する個別情報取得手段と、取得された前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手段と、取得された個別情報と番組情報とを組にして暗号化して出力する暗号化手段と、

番組データ及び前記暗号化手段によって得られた暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手段と、

前記番組情報と前記個別情報とに基づいて、番組データの視聴の可否を判定するものであって、

前記記録手段から再生された番組データに含まれる番組情報が前記復号化手段によって得られた個別情報中のワーク鍵を用いて復号化されて番組情報が得られ、得られた番組情報と前記復号化手段によって得られた番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手段とを具備したことを特徴とする有料放送タイムシフト視聴方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、スクランブルされた有料放送番組をそのまま記録し再生時にデスクランブル処理して視聴する有料放送システム、有料放送受信機及び有料放送タイムシフト視聴方法に関する。

【0002】

【従来の技術】従来、衛星（BS）を用いた有料のデジタル放送が行われている。有料のBSデジタル放送では、放送する番組にスクランブルが施される。視聴者は、放送局と契約することによってスクランブルを解除するスクランブル鍵が与えられる。スクランブル鍵を用いて受信信号をデスクランブルすることにより、番組の視聴が可能となる。

【0003】放送局では、スクランブル鍵を放送信号に多重して送信する。この場合には、スクランブル鍵は、番組の視聴条件等に関する情報と共にECM (Entitlement Control Message) として送信される。

【0004】一方、視聴者側の受信機は、受信信号をデスクランブルするデスクランブラを有していると共に、デスクランブルに必要なスクランブル鍵を発生するためのカードユニット (ICカード) を備えている。ICカードは、番組の視聴可能な期限等契約条件の情報を含む個別情報 (以下、EMM (Entitlement Management Message) という) を保持している。なお、EMMは放送局から送信されて、ICカード内に取込まれることもある。

【0005】ICカード内においては、受信信号に含まれるECMからスクランブル鍵を取得し、ECMと保持しているEMMとから各番組毎に視聴の可否を判定する。ICカードからは、番組視聴可の場合にのみスクランブル鍵がデスクランブラに供給される。これにより、契約条件によって視聴が許可された番組のみが視聴可能となる。

【0006】ところで、有料放送においても、放送番組をいったん記録し、後に再生して視聴することが考えられる。この場合には、著作権保護の観点から、記録する番組についてはスクランブルをかけたまま記録を行う。ところが、放送局によってEMMが変更されることがある。放送局から変更されたEMMが送信されると、受信機側のICカード内のEMMは更新される。記録されているEMM変更前の有料放送番組については、変更後のEMMを用いて復号することができないことがある。

【0007】そこで、番組放送時点におけるEMMを放送番組と共に記録装置に記録することが考えられる。ICカードにEMMの入出力機能を付加すると共に、このようなタイムシフト視聴であるかりアルタイム視聴であるかを判断して、番組の復号に用いるEMMを記録装置から再生したものとICカード内に保持しているものとで切換えるのである。

【0008】しかしながら、有料放送のこのようなタイムシフト視聴においては、不正視聴が行われることが考えられる。図3乃至図5は不正視聴の例を説明するための説明図である。図3乃至図5は水平方向に時間の経過をとり、また、斜線によって非契約であること及び本来視聴が許可されていない番組であることを示している。

【0009】図3は放送局と視聴契約していない時点で放送された番組Aを記録し、契約後に番組Aを再生する例を示している。図3中の番組Aは視聴契約していない番組であり、番組Bは視聴契約している番組である。また、EMMは契約前後で変化しないものとし、番組Bに対応したEMMで番組Aも復号可能であるものとする。

【0010】視聴契約前に番組Aを記録する時点では、まだ視聴契約が行われていないので、EMMを番組と同時

時に記録することはできない。しかし、視聴契約を行えば、番組Bの受信時にはEMMを取得することができる。そして、受信機を改造して、再生した番組Aをリアルタイム視聴した番組としてICカードに供給することにより、契約後に得られたICカード内のEMMを使用して番組Aを復号することができる。あるいは、ICカードを制御するコマンドによって、記録装置から再生した番組の復号時であってもICカード内のEMMを使用するように制御することによっても、契約後に得られたICカード内のEMMを使用して番組Aを復号することができる。

【0011】図4中の番組Aは視聴契約していない番組であり、番組Bは視聴契約している番組である。また、EMMは契約前後で変化しないものとする。

【0012】視聴契約前に番組Aを記録する。この時点ではEMMを同時に記録することはできない。その後契約を行うことによって、番組Bの受信時にEMMを取得することができる。

【0013】図4に示すように、図3と同様の契約状況において、その後、再び契約を解除するものとする。この場合でも、番組Bについては視聴契約があるので、契約時に記録した番組Bをタイムシフト視聴することは問題はない。しかし、図3の不正視聴と同様の手法によって、非契約となった後においても、番組B記録時に記録したEMMを利用することで、番組Aを復号することが可能となる。

【0014】図5は特定の番組の視聴契約であるスペシャル契約を一時期行った後、通常のベーシック契約に変更した場合の例である。契約の変更前後においてEMMは変化しないものとする。

【0015】スペシャル契約時に番組Bと共にEMMを記録装置に記録する。その後契約をベーシック契約に変更し、ベーシック契約となった以降の番組Cを記録する。この場合でも、番組BのEMMによって番組Cの復号が可能であるものとする。図3の不正視聴と同様の手法によって、スペシャル契約時に記録したEMMを利用して、ベーシック契約後に記録した番組Cの復号が可能である。

【0016】

【発明が解決しようとする課題】このように、従来、タイムシフト視聴では、視聴契約した番組に対応していないEMMを利用して不正視聴されてしまうことがあるという問題点があった。

【0017】本発明はかかる問題点に鑑みてなされたものであって、タイムシフト視聴を可能にした場合でも、不正視聴を確実に防止することができる有料放送システム、有料放送受信機及び有料放送タイムシフト視聴方法を提供することを目的とする。

【0018】

【課題を解決するための手段】本発明の請求項1に係る

有料放送システムは、番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報を暗号化するために用いられるワーク鍵と、視聴契約の内容に応じた情報と、を含む個別情報であって、前記視聴契約の開始及び終了時の情報を含む個別情報を生成する個別情報生成手段を具備したものであり、本発明の請求項2に係る有料放送受信機は、番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信手段と、前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する視聴可否判定手段とを具備したものであり、本発明の請求項3に係る有料放送受信機は、番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する受信手段と、前記受信手段が受信した個別情報を取得する個別情報取得手段と、前記個別情報取得手段が取得した前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手段と、前記個別情報取得手段が取得した個別情報と前記番組情報取得手段が取得した番組情報とを組にして暗号化して出力する暗号化手段と、前記受信手段が受信した番組データ及び前記暗号化手段からの暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手段と、前記番組情報と前記個別情報とに基いて、番組データの視聴の可否を判定するものであって、前記記録手段が再生した番組データに含まれる番組情報を前記番組情報取得手段が前記復号化手段からの個別情報中のワーク鍵を用いて復号化して得た番組情報と前記復号化手段からの番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手段とを具備したものであり、本発明の請求項5に係る有料放送タイムシフト視聴方法は、番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信手段と、前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する手順とを具備したものであり、本発明の請求項6に係る有料放送タイムシフト視聴方法は、番組データと、前記番組データのスクラ

ンブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する手順と、受信した個別情報を取得する個別情報取得手段と、取得された前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手段と、取得された個別情報と番組情報とを組にして暗号化して出力する暗号化手段と、番組データ及び前記暗号化手段によって得られた暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手段と、前記番組情報と前記個別情報とに基いて、番組データの視聴の可否を判定するものであって、前記記録手段から再生された番組データに含まれる番組情報が前記復号化手段によって得られた個別情報中のワーク鍵を用いて復号化されて番組情報が得られ、得られた番組情報と前記復号化手段によって得られた番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手段とを具備したものである。

【0019】本発明の請求項1において、個別情報生成手段は、視聴契約の開始及び終了時の情報を含む個別情報を生成する。これにより、受信側で、視聴契約の終了時だけでなく開始時の情報を利用した視聴可否の判定を可能にする。

【0020】本発明の請求項2において、受信手段は、番組データ、番組情報及び個別情報を受信する。個別情報には、視聴契約の開始及び終了時の情報が含まれる。視聴可否判定手段は、視聴契約の終了時の情報だけでなく、開始時の情報を用いて、番組データの視聴の可否を判定する。

【0021】本発明の請求項3において、受信手段は、番組データ、番組情報及び個別情報を受信する。個別情報取得手段が取得した個別情報と番組情報取得手段が取得した番組情報とは、暗号化手段によって、組にされて暗号化される。記録された番組データをタイムシフト視聴する場合には、組にされて暗号化された個別情報及び番組情報は、復号化手段によって復号される。再生された番組データに含まれる番組情報は、番組情報取得手段によって、復号化手段からの個別情報を用いて復号化される。判定手段は、番組情報取得手段からの番組情報と復号化手段からの番組情報との同一性を判定する。判定手段は、同一でない場合には、視聴不可と判定し、同一であると判定した場合にのみ、番組情報と個別情報とに基く視聴可否の判定を有効とする。

【0022】本発明の請求項5において、前記視聴契約の開始及び終了時の情報を含む個別情報を受信する。この視聴契約の開始及び終了時の情報を用いて、番組デー

タの視聴の可否を判定する。

【0023】本発明の請求項6において、番組データと、番組情報と、個別情報とを受信する。受信した個別情報を取得し、取得された個別情報中のワーク鍵を用いて番組情報を復号化する。暗号化手順では、取得された個別情報と番組情報とを組にして暗号化して出力する。記録手段に記録された番組データを再生してタイムシフト視聴する場合には、復号化手順は、暗号化された個別情報と番組情報との組を復号化して個別情報及び前記番組情報の組を取得する。復号された個別情報を用いて、再生された番組データに含まれる番組情報を復号化する。番組情報と復号化手順による番組情報とについては、視聴可否判定手順において同一性を判定する。同一でない場合には、視聴不可と判定し、同一であると判定した場合にのみ、番組情報と個別情報とに基く視聴可否の判定が有効となる。

【0024】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。図1は本発明の一実施の形態に係る有料放送システム及び有料放送受信機を示すブロック図である。

【0025】放送局1は有料放送の放送信号を送信する。番組を構成する映像信号及び音声信号等は例えばMPEG規格で符号化され、番組のトランスポートストリーム(Transport Stream)がTV(テレビジョン)信号としてスクランブル部4に供給される。放送局1は、有料の放送番組にはスクランブルを施す。スクランブル部4は、入力されたTV信号に対して所定のスクランブル鍵を用いたスクランブル処理を施して多重化部7に与える。

【0026】有料放送においては、視聴者は、放送局と視聴契約を結ぶことによって、有料放送番組を受信して視聴することができる。受信側では、契約条件等に応じて、視聴可と判定された番組については、スクランブル鍵を用いてデスクランブル処理することによって、有料放送番組の視聴を行う。このような視聴可否の判定をICカードを用いて行うことがある。

【0027】例えば、日本のCSを利用した放送であるスカイパーフェクTVやディレクTV等の放送を受信する機器においては、視聴可否の判定にICカードが利用されている。ICカードは、カードを識別するためのカードID及びカード毎に固有のマスター鍵K_mを記憶している。ICカードは、後述するように、マイコン装置であり、マイコン内の不揮発メモリに契約条件等の情報を記憶し、番組受信時に番組の情報と契約条件等の情報とに基いて視聴可否を判定するのである。

【0028】このような視聴可否の判定のために、ECM及びEMMが用いられる。ECMは、社団法人電波産業会が策定したBSデジタル放送限定受信方式の標準規格のARIB STD-B25 1.0版(以下、標準

規格という)にて規定されている。この規定によれば、ECMは、常に固定的に伝送される固定部と、目的によって内容が異なる可変部とによって構成される。ECM固定部には、プロトコル番号、有料事業体識別、ワーク鍵識別、番組に施したスクランブルのスクランブル鍵、判定タイプ、年月日時分、録画制御及び改ざん制御が配置される。また、ECM可変部には、ティア(定額)判定に関する機能情報、従量課金(PPV(ペイパービュー))判定に関する機能情報及び消去に関する機能情報が配置される。即ち、ECMによって、番組を特定する情報及び録画の可否等を示す情報が伝送される。

【0029】また、EMMについても、標準規格にて規定されている。この規定によれば、EMMは、常に固定的に伝送される固定部と、目的によって内容が異なる可変部とによって構成される。EMM可変部には、各種機能情報、即ち、ワーク鍵に関する機能情報、ティアに関する機能情報、後払いPPVに関する機能情報、通電制御に関する機能情報、全体制御に関する機能情報及び強制発呼に関する機能情報が配置される。また、EMM固定部には、カードID、関連情報バイト長、プロトコル番号、有料事業体識別、更新番号及び契約の終了時を示す有効期限の情報が配置される。EMMのうちカードIDを除く部分については後述するように暗号化されるようになっている。

【0030】ECM生成/暗号化部5は、番組毎にECMを生成する。上述したように、ECMにはスクランブル鍵が含まれており、ECM生成/暗号化部5は、ワーク鍵K_wを用いて、生成したECMを暗号化した後、多重化部7に出力するようになっている。受信側では、ワーク鍵K_wを用いることで、ECMを復号化してスクランブル鍵を得ることができる。

【0031】放送局1は、視聴契約が変更されること及び不正視聴を防止するために、ワーク鍵K_wを適宜変更するようになっている。このため、放送局1は、ワーク鍵K_wについても、多重化して送信するようになっている。上述したように、EMM可変部にワーク鍵K_wに関する情報を配置する。

【0032】EMM生成/暗号化部6は、EMMを生成するようになっている。EMM生成/暗号化部6は、視聴契約に応じて、EMMを個別の宛先に送信する。即ち、EMM生成/暗号化部6は、EMM固定部に、非暗号のカードIDを配置することで、受信側が自己宛のEMMを識別することを可能にする。カードIDは視聴契約に際して放送局1に与えられる。

【0033】即ち、視聴者が放送局1との間で視聴契約を結ぶ場合には、視聴者は受信機に取り付けるICカードの情報を放送局1に与えるようになっている。放送局1は、視聴者情報蓄積部2において、ユーザーとID、IDとマスター鍵K_mとの関係を記述した視聴者情報を保持している。視聴者管理部3は、視聴契約に応じて視

聴情報蓄積部2に保持する視聴者情報を更新すると共に、各ユーザー毎のID及びマスター鍵 K_m を讀出してEMM生成/暗号化部6に出力するようになっている。

【0034】本実施の形態においては、EMM生成/暗号化部6は、EMM固定部に配置する有効期限に関する情報に、契約の開始を示す情報を加えるようになっている。EMM生成/暗号化部6は、契約の開始及び終了時を示す情報を含むEMM固定部とワーク鍵 K_w や契約条件を含むEMM可変部とを生成し、カードIDを除く部分についてはマスター鍵 K_m を用いて暗号化する。EMM生成/暗号化部6からのEMMは多重化部7に供給される。

【0035】多重化部7は、スクランブル部5の出力、ECM生成/暗号化部5の出力及びEMM生成/暗号化部6の出力を多重化して、アンテナ8から送信するようになっている。アンテナ8からの放送信号は衛星9によって放送される。

【0036】一方、有料放送受信機10においては、衛星9からの放送信号をアンテナ11によって受信する。アンテナ11からの高周波信号は選局回路12に供給され、選局回路12は、システムコントローラ29から指示されたチャンネルの番組を選択して、番組データを出力する。選局回路12の出力は、切り替え回路13に供給されると共に、端子32を介して記憶装置35にも供給される。

【0037】なお、システムコントローラ29はユーザー操作に基いて選局チャンネルを切替える。ユーザーは例えばリモコン31によって有料放送受信機10を制御する。リモコン31は、ユーザー操作に基く信号を送信し、リモコン受信部30は、リモコン31からの信号を受信してシステムコントローラ29に与える。これにより、システムコントローラ29は、ユーザー操作に基いて、有料放送受信機10の各部を制御するようになっている。

【0038】記録装置35は、端子32を介して選局回路12からの番組データが与えられ、ユーザー操作に応じて入力された番組データを所定の記録媒体に記録する。また、記録装置35は、記録媒体に記録されている番組データを再生して、端子33を介して有料放送受信機10に出力することができるようになっている。

【0039】更に、記録装置35は、端子34を介して有料放送受信機10に接続されており、有料放送受信機10に挿着されたICカード19内のEMM暗号化/復号化部28からのEMM信号を、選局回路12からの番組データに対応させて記録媒体に記録すると共に、記録されたEMM信号を再生してEMM暗号化/復号化部28に出力することができるようになっている。

【0040】なお、記録装置35としては種々の装置を利用可能である。例えば、DVD、ハードディスク等を利用した機器、デジタルVTR等種々考えられる。また、受信機10と記録装置35との間の接続についても

規定しない。

【0041】また、スクランブルされた番組を入出力する端子32、33とEMMを入出力する端子34とを別々のものとしたが、番組にEMMを多重した形で出力する場合も考えられる。

【0042】切り替え回路13は、放送番組を視聴する場合には、選局回路12の出力を選択して分離回路14に与え、記録している番組を視聴する場合には、端子33からの記録装置35の出力を選択して分離回路14に与えるようになっている。分離回路14は、入力された番組データ中に含まれる番組のストリーム、ECM及びEMMを分離し、夫々、デスクランブラ15、ICカード19及びフィルタリング部17に出力する。

【0043】デスクランブラ15は、後述するように、ICカード19からデスクランブル鍵が与えられて、入力されたストリームをデスクランブル処理してMPEGデコーダ16に出力する。MPEGデコーダ16は、入力されたトランスポートストリームをデコードして、番組の映像信号及び音声信号等(TV信号)を図示しないモニタに出力するようになっている。

【0044】ICカード19は、カードIDを図示しない記憶部に記憶している。ID読出し部18は、ICカード19からカードIDを讀出して、フィルタリング部17に供給するようになっている。フィルタリング部17は、分離回路14から与えられたEMMに含まれるカードIDとID読出し部18からのカードIDとを比較することによって、自機宛のEMMを識別する。フィルタリング部17は、自機宛のEMMは、ICカード19に出力するようになっている。

【0045】分離回路14からのECMは、ICカード19のECM復号化部21に与えられ、フィルタリング部17からのEMMはEMM復号化部22に与えられる。ICカード19は、マスター鍵 K_m を格納している K_{mi} メモリ23を有している。EMM復号化部22は K_{mi} メモリ23からのマスター鍵 K_m を用いてEMMを復号化する。これにより、EMMに含まれるワーク鍵 K_w 及びその他の情報が得られる。EMM復号化部22は、復号したEMM(ワーク鍵 K_w を含む)をEMMメモリ24に出力すると共に、ワーク鍵 K_w をECM復号化部21に出力する。

【0046】ECM復号化部21は、EMM復号化部22又は後述するEMM暗号化/復号化部28からのワーク鍵 K_w を用いて、分離回路14からのECMを復号化する。これにより、ECMに含まれるスクランブル鍵及びその他の情報が得られる。ECM復号化部21の復号出力は視聴可否判定部26に与えられる。

【0047】EMMメモリ24は入力されたEMMを保持し、放送局1によってEMMが更新されるまで、保持しているEMMをEMM復号化部22に与えると共に、セレクト25を介して視聴可否判定部26に与える。ま

た、EMMメモリ24は保持しているEMMをEMM暗号化/復号化部28にも出力するようになっている。EMM暗号化/復号化部28はEMMメモリ24からのEMMを暗号化して、端子34から記憶装置35に供給するようになっている。また、EMM暗号化/復号化部28は、記憶装置35から再生されたEMMが端子34を介して入力され、入力されたEMMを復号化して復号出力をセクタ25に出力すると共に、復号出力に含まれるワーク鍵KwをECM復号化部21に出力するようになっている。

【0048】セクタ25は、リアルタイム視聴時にはEMMメモリ24からのEMMを選択し、タイムシフト視聴時にはEMM暗号化/復号化部28からのEMMを選択して視聴可否判定部26に出力する。

【0049】視聴可否判定部26は、入力されたECMとEMMとを対比し、デスクランブラに入力された番組データが視聴許可されているか否かを判定する。視聴可否判定部26は、視聴可であると判定した場合には、ECM復号化部21からのスクランブル鍵をデスクランブル鍵としてデスクランブラ15に与える。視聴可否判定部26は、視聴不可と判定した場合には、スクランブル鍵を出力しない。従って、この場合には、デスクランブラ15はデスクランブル処理を行うことができず、番組を正常に視聴することはできない。

【0050】本実施の形態においては、視聴可否判定部26は、視聴可否の判定に際して、視聴契約の期限の情報、即ち、視聴契約の終了時の情報だけでなく、視聴契約の開始時の情報も用いるようになっている。即ち、視聴可否判定部26は、入力されたEMM中の視聴契約開始時の情報によって示される視聴契約開始時がECMによって示される番組の放送日時よりも前でない場合には、視聴不可と判定するようになっている。つまり、視聴可否判定部26は、入力されたEMM中の視聴契約開始及び終了時の情報によって示される視聴契約開始から終了までの間に、ECMによって示される番組の放送が行われている場合にのみ視聴可と判定する。

【0051】視聴可否判定部26は、視聴可と判定した場合には、視聴情報メモリ27に視聴情報を出力するようになっている。PPV（ペイパービュー）では、番組毎に購入、非購入を決定することができる。視聴情報メモリ27は、購入した（視聴した）PPVの番組を特定するための情報を視聴情報として記憶するようになっている。なお、視聴情報メモリ27に格納された視聴情報は、図示しない電話回線等によって、放送局に伝送され、視聴料の精算に用いられる。

【0052】次に、このように構成された実施の形態の動作について説明する。

【0053】放送局1は、スクランブル部4によって番組ストリームにスクランブルをかける。ECM生成/暗号化部5はスクランブル鍵を含むECMを生成して、ワ

ーク鍵Kwによって暗号化する。視聴者情報蓄積部2は、各ユーザ、カードID及びマスター鍵Kmの情報を含む視聴者情報を蓄積している。EMM生成/暗号化部6は、所定のタイミングで、ワーク鍵Kw及びカードIDを含むEMMを作成し、カードIDを除く部分をマスター鍵Kmを用いて暗号化する。

【0054】本実施の形態においては、EMM生成/暗号化部6は、EMM固定部には、視聴契約の開始及び終了時を示す期限情報を配置する。スクランブルが施された番組ストリーム及び暗号化されたECM、EMMは、多重化部7において多重化され、アンテナ8から送信される。

【0055】一方、受信側においては、アンテナ11を介して受信した放送信号は、選局回路12によって所定チャンネルの番組が選局される。いま、リアルタイム視聴を行うものとする。この場合には、切り替え回路13は選局回路12の出力を選択して分離回路14に出力する。分離回路14によって、切り替え回路13の出力に含まれる番組データ、ECM、EMMは、夫々デスクランブラ15、ECM復号化部21及びフィルタリング部17に供給される。

【0056】ID読出し部18は、ICカード19からカードIDを讀出してフィルタリング部17に供給する。フィルタリング部17は、カードIDを比較することによって、分離回路14の出力から自機宛のEMMをフィルタリングしてICカード19に出力する。

【0057】ICカード19のEMM復号化部22は、Kmiメモリ23からマスター鍵Kmを讀出して、ICカード19に入力されたEMMを復号し、EMMメモリ24に出力する。また、EMM復号化部22はEMMに含まれるワーク鍵KwをECM復号化部21に与える。このワーク鍵Kwを用いて、ECM復号化部21は、分離回路14からのECMを復号する。これにより、ECM復号化部21はスクランブル鍵を含むECMを得て視聴可否判定部26に出力する。

【0058】なお、放送局1からの放送信号に自機宛のEMMが含まれない場合には、EMM復号化部22はEMMメモリ24に格納されているEMM中のワーク鍵KwをECM復号化部21に出力する。

【0059】セクタ25はEMMメモリ24からのEMMを視聴可否判定部26に出力する。視聴可否判定部26は、ECMとEMMとに基いて、デスクランブラ15に入力されている番組データが視聴可の番組のものであるか否かを判定する。ユーザがリモコン31で視聴を希望したチャンネル（番組）は、視聴契約によって視聴が許可されているものであるものとする。視聴可否判定部26は、スクランブラ15に入力されている番組データが視聴可の番組のものであるものと判定し、ECMに含まれるスクランブル鍵をデスクランブル鍵としてデスクランブラ15に出力する。

【0060】デスクランブラ15は、デスクランブル鍵を用いて番組データのスクランブルを解除する。デスクランブラ15からの番組ストリームはMPEGデコーダ16に供給され、デコードされてTV信号が得られる。このTV信号をモニタに供給することによって、ユーザが指定した番組の視聴が可能となる。

【0061】また、ユーザが指定した番組が視聴契約されていない場合には、視聴可否判定部26は、ECM、EMMから視聴不可であるものと判定し、スクランブル鍵を出力しない。従って、この場合には、ユーザが指定した番組のデスクランブル処理は行われず、番組を正常に視聴することはできない。

【0062】なお、視聴可否判定部26は、視聴可否の判定を行った番組がPPVである場合には、視聴情報を視聴情報メモリ27に格納する。

【0063】次に、ユーザが番組の記録を指示するものとする。この場合には、選局回路12からの番組データは、端子32を介して記録装置35に供給され、記録媒体上に記録される。

【0064】また、切り替え回路13は選局回路12の出力を分離回路14に与える。こうして、番組の記録時においても、EMMがフィルタリング部17からICカード19に供給される。EMM復号化部23は、Kmメモリ23から読出したマスター鍵Kmを用いてEMMを復号し、復調出力をEMMメモリ24に出力する。EMMメモリ24はEMM復号化部22の出力によって記録しているEMMを更新する。なお、自機宛のEMMが放送されない場合には、EMMメモリ24は保持しているEMMを更新しない。

【0065】番組の記録時には、EMMメモリ24は保持しているEMMをEMM暗号化／復号化部28に出力する。EMM暗号化／復号化部28は、入力されたEMMを暗号化してICカード19から出力する。暗号化されたEMMは端子34から記録装置35に供給され、記録装置35は暗号化されたEMMを対応する番組データと共に記録媒体に記録する。

【0066】次に、ユーザが記録装置35に記録されている番組を再生して視聴するものとする。この場合には、システムコントローラ29は、切り替え回路13に記録装置35の出力を選択させると共に、セレクト25にEMM暗号化／復号化部28の出力を選択させる。記録装置35からの番組データは切り替え回路13を介して分離回路14に供給される。また、記録装置35から再生された番組データに対応するEMMは、端子34からICカード19内のEMM暗号化／復号化部28に供給される。EMM暗号化／復号化部28は再生されたEMMを復号して出力する。

【0067】分離回路14は、再生出力中の番組データをデスクランブラ15に出力し、ECMをECM復号化部21に出力する。ECM復号化部21は、EMM暗号

化／復号化部28からのEMMに含まれるワーク鍵Kwを用いて、ECMを復号化する。ECM復号化部21は復号したECMを視聴可否判定部26に出力する。セレクト25はEMM暗号化／復号化部28からのEMMを視聴可否判定部26に出力する。

【0068】このように、視聴可否判定部26には、番組放送当時の番組に対応したECMとこの番組に対応したEMMとが入力される。視聴可否判定部26は入力されたECM、EMMから視聴可否を判定する。番組放送当時に、記録した番組についての視聴契約が結ばれている場合には、視聴可否判定部26は入力されたECM、EMMから視聴可と判定することができる。逆に、記録した番組についての視聴契約が結ばれていない場合には、視聴可否判定部26は入力されたECM、EMMから視聴不可と判定することができる。こうして、記録装置35に記録された番組をタイムシフト視聴する場合においても、視聴契約に応じた視聴が行われる。

【0069】また、視聴契約を途中で変更した場合、例えば、ある月の月末に記録した番組を、翌日(翌月)に視聴する場合において、その月変わりて契約を変更し、翌月から記録した番組を放送するチャンネルの契約が無くなる場合等であっても、記録した番組とこの番組に対応するEMMを視聴可否の判定に用いることができるので、正常にタイムシフト視聴が可能である。

【0070】ここで、ユーザの不正によって、記録装置35から再生された番組と対応しないEMMが視聴可否判定部26に入力されるものとする。例えば、番組A、B等に対する視聴契約が図3又は図4に示す状況であるものとし、視聴契約が結ばれていない番組Aの再生時に、視聴契約された番組Bに対応するEMMが視聴可否判定部26に入力されるものとする。なお、番組Bに対応するEMMは、従来と同様の視聴可否の判定方法によれば、番組Aの復号を可能にするものとする。即ち、番組Bに対応するEMMは、ワーク鍵Kwが番組Aに用いられたものと同一であり、また、視聴契約の終了時は番組Aの放送日時よりも後に設定されている。

【0071】しかし、視聴可否判定部26は、EMMに含まれる視聴契約の開始時の情報も用いて視聴可否を判定する。即ち、図3及び図4の場合には、番組Bに対応するEMM中には、視聴契約の開始時が番組Aの放送日時よりも後の日時を示す情報が記述されていることから、視聴可否判定部26は、番組Aに対応するECMと番組Bに対応するEMMとが入力された場合でも、番組Aについては視聴不可と判定する。

【0072】これにより、視聴契約を行っていない番組Aについては、対応していないEMMを用いた不正視聴をユーザが試みても、正常にタイムシフト視聴することはできない。

【0073】このように、本実施の形態においては、EMM内の視聴契約の期限情報として、視聴契約の終了時

だけでなく開始時の情報も含めて送信し、ECM内の時刻情報と比較してEMMの視聴契約の始まりを示す情報が時間的に前であり、かつ契約の終わりを示す時刻情報が時間的に後であることを条件に視聴可とするようにしているので、ユーザが再生する番組に対応していないEMMを不正に利用してタイムシフト視聴しようとしても、視聴を不許可にすることができ、不正視聴を防止することができる。

【0074】図2は本発明の他の実施の形態を示すブロック図である。図2において図1と同一の構成要素には同一符号を付して説明を省略する。図1の実施の形態においては、図5の場合については不正視聴を阻止することはできない。本実施の形態においては図3乃至図5のいずれの場合においても不正視聴を阻止可能にしたものである。なお、図2においては受信機側の構成のみを示したが、放送局側の構成は、図1に示すものと同一であってもよく、また、従来と同一であってもよい。即ち、本実施の形態においては、EMM中に視聴契約の開始時の情報を含めなくても不正視聴を阻止することができる。

【0075】図2において、有料放送受信機45は、ICカード19に代えてICカード40を採用した点が図1の有料放送受信機10と異なる。ICカード40は、EMM暗号化/復号化部28に代えてEMMとECM暗号化/復号化部41を採用し、視聴可否判定部26に代えて視聴可否判定部42を採用した点がICカード19と異なる。

【0076】EMMとECM暗号化/復号化部41には、EMMメモリ24からEMMが入力されるだけでなく、ECM復号化部21から復号されたECMも入力されるようになっている。EMMとECM暗号化/復号化部41は、入力されたECM、EMMを組み合わせて暗号化し、暗号化したECM、EMMを端子34を介して記録装置35に出力するようになっている。ECM、EMMが組み合わされて暗号化されていることから、復号化しなければ、ECM、EMMを取り出すことはできない。即ち、ECM、EMMの一方のみを、復号化せずに取り出すことはできない。

【0077】記録装置35は、端子34からのECM、EMMを番組データに対応させて記録媒体に記録する。記録装置35は、番組データの再生時には、対応するECM、EMMを再生して端子34からICカード40に供給するようになっている。

【0078】EMMとECM暗号化/復号化部41は、端子34を介して入力されたECM、EMMを復号化し、セレクト25を介して視聴可否判定部42に出力すると共に、復号化したEMM中のワーク鍵 K_w をECM復号化部21に供給するようになっている。

【0079】視聴可否判定部42は、再生時には、EMMとECM暗号化/復号化部41からのEMM及びEC

Mを視聴可否の判定に用いる。即ち、視聴可否判定部42は、EMMとECM暗号化/復号化部41からのECMとECM復号化部21からのECMとの一致を検出し、一致している場合にのみ視聴可否の判定が正当であるものとし、そうでない場合には、視聴不可の判定を行うようになっている。

【0080】上述したように、ECM内には、EMMの契約の期限と比較判定するための日時情報（年月日時分秒等）が含まれている。視聴可否判定部42は、例えば、日時情報内の所定部分が一致することによって同一性を判定する。例えば、日時情報中の年月の情報を用いる。この場合には、1ヶ月内の不正視聴を阻止することができるが、契約の単位が1月単位であれば十分である。更に、例えば、年月日又は年月日時まで判定することによって、一層厳密な同一性判定が可能となる。例えば、視聴契約が日毎で変更可能な場合には、年月日を同一性判定の基準にすると、その日内の番組に対して不正視聴の危険性がある。システムを適用する放送局の意向に従って、同一性判定のための判定基準を設定すればよい。

【0081】次に、このように構成された実施の形態の動作について説明する。

【0082】録画時には、選局回路12からスクランブルされたままの番組データを記録装置32に供給する。また、EMMとECM暗号化/復号化部41には、EMMメモリ24及びECM復号化部21から、記録する番組に対応したEMMとECMとが入力される。EMMとECM暗号化/復号化部41は、入力されたECM、EMMを組にして、組となったECM、EMMを暗号化する。EMMとECM暗号化/復号化部41の出力は、端子34を介して記録装置35に供給され、番組と共に記録される。

【0083】再生時には、記録装置35は、スクランブルされた番組データを端子33を介して切り替え回路13に出力すると共に、暗号化されたECM、EMMの組を端子34を介してICカード40のEMMとECM暗号化/復号化部41に出力する。

【0084】EMMとECM暗号化/復号化部41は暗号化されているECM、EMMを復号し、ECM、EMMの組をセレクト25を介して視聴可否判定部42に出力する。また、EMMとECM暗号化/復号化部41は、ECMMをECM復号化部21にも出力する。ECM復号化部21は、分離回路14から再生番組中のECMが与えられ、EMM中のワーク鍵 K_w を用いて復号化し、復号したECMを視聴可否判定部42に出力する。

【0085】視聴可否判定部42は、再生する番組についての視聴可否を判定する場合には、EMMと組になって入力されたECMがECM復号化部21からのECMに一致するか否かを判定する。視聴可否判定部42は、入力された2つのECMを一致と判定した場合にのみ、

視聴可否判定を有効とし、そうでない場合には、視聴不可と判定する。

【0086】ここで、ユーザの不正によって、記録装置35から再生された番組と対応しないEMM、ECMの組がICカード40に入力されるものとする。この場合でも、例えば、番組B、C等に対する視聴契約が図5に示す状況であるものとし、視聴契約が結ばれていない番組Cの再生時に、視聴契約された番組Bに対応するEMMとECMの組がICカード40に入力されるものとする。なお、番組Bに対応するEMMは、従来と同様の視聴可否の判定方法によれば、番組Cの復号を可能にするものとする。

【0087】この場合においても、ECM復号化部21は、EMMとECM暗号化／復号化部41からのEMMを用いて、ECMを復号化可能である。しかし、視聴可否判定部42は、ECM復号化部21からのECMとEMMとECM暗号化／復号化部41からのECMとの一致を判定する。ECMは番組を特定する情報を有しているので、視聴可否判定部42は、EMMとECM暗号化／復号化部41からのECMとECM復号化部21からのECMが不一致であることを判定することができる。

【0088】視聴可否判定部42は、入力された2つのECMが不一致であると判定したことにより、ICカード40に入力された再生番組の視聴は不可であるものと判定する。即ち、この場合には、デスクランブラ15にはデスクランブル鍵は供給されない。

【0089】なお、本実施の形態によれば、EMMに視聴契約開始時の情報を含めることなく、図3及び図4の例においても、不正視聴を防止することができることは明らかである。

【0090】このように、本実施の形態においては、EMMとECMとを組にして暗号化し、再生番組の復号にEMMを用いる場合には、このEMMと組になったECMもICカード40に取込むようになっており、入力される番組データから得たECMと記録装置35から得たECMとの一致判定を行うことで、不正視聴を確実に防止することができる。

【0091】なお、視聴可否判定部42の同一性判定の手法としては種々の手法が考えられる。例えば、ECM内に番組番号を配置し、これを利用してもよい。番組番号を、いわゆる番組毎に割り当てることにより、ECMの一致比較から他の番組用のEMMを復号に利用することができなくなる。

【0092】また、同一性判定のその他の方法として、ECM内に含まれるデスクランブル鍵以外の情報が一致するか否かを判定するようにしてもよい。更に、ECMの判定の細かさを、ECMで指定してもよい。すなわち、番組再生時に、ECMで指定された細かさにより、同一性判定の方法を変えるのである。ICカード40内に入力される番組データのECMに、同一性判定の方法として日時情報を使用し、細かさが年月までとなっている場合には、同一性判定の方法として番組番号を使用する場合など指定する。このようにすることによって、放送局の意向を番組毎に反映させた判定が可能となる。

【0093】

【発明の効果】以上説明したように本発明によれば、タイムシフト視聴を可能にした場合でも、不正視聴を確実に防止することができるという効果を有する。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係る有料放送システム及び有料放送受信機を示すブロック図。

【図2】本発明の他の実施の形態を示すブロック図。

【図3】従来例における問題点を説明するための説明図。

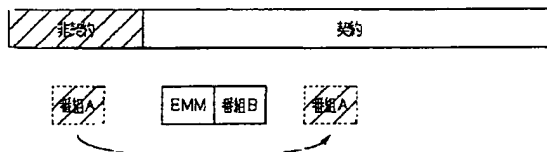
【図4】従来例における問題点を説明するための説明図。

【図5】従来例における問題点を説明するための説明図。

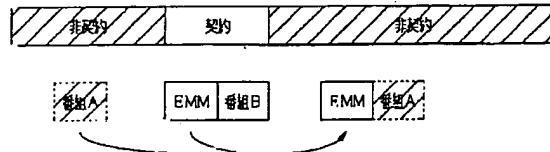
【符号の説明】

1…放送局、6…EMM生成／暗号化部、10…有料放送受信機、15…デスクランブラ、19…ICカード、21…ECM復号化部、22…EMM復号化部、26…視聴可否判定部、28…EMM暗号化／復号化部、35…記録装置。

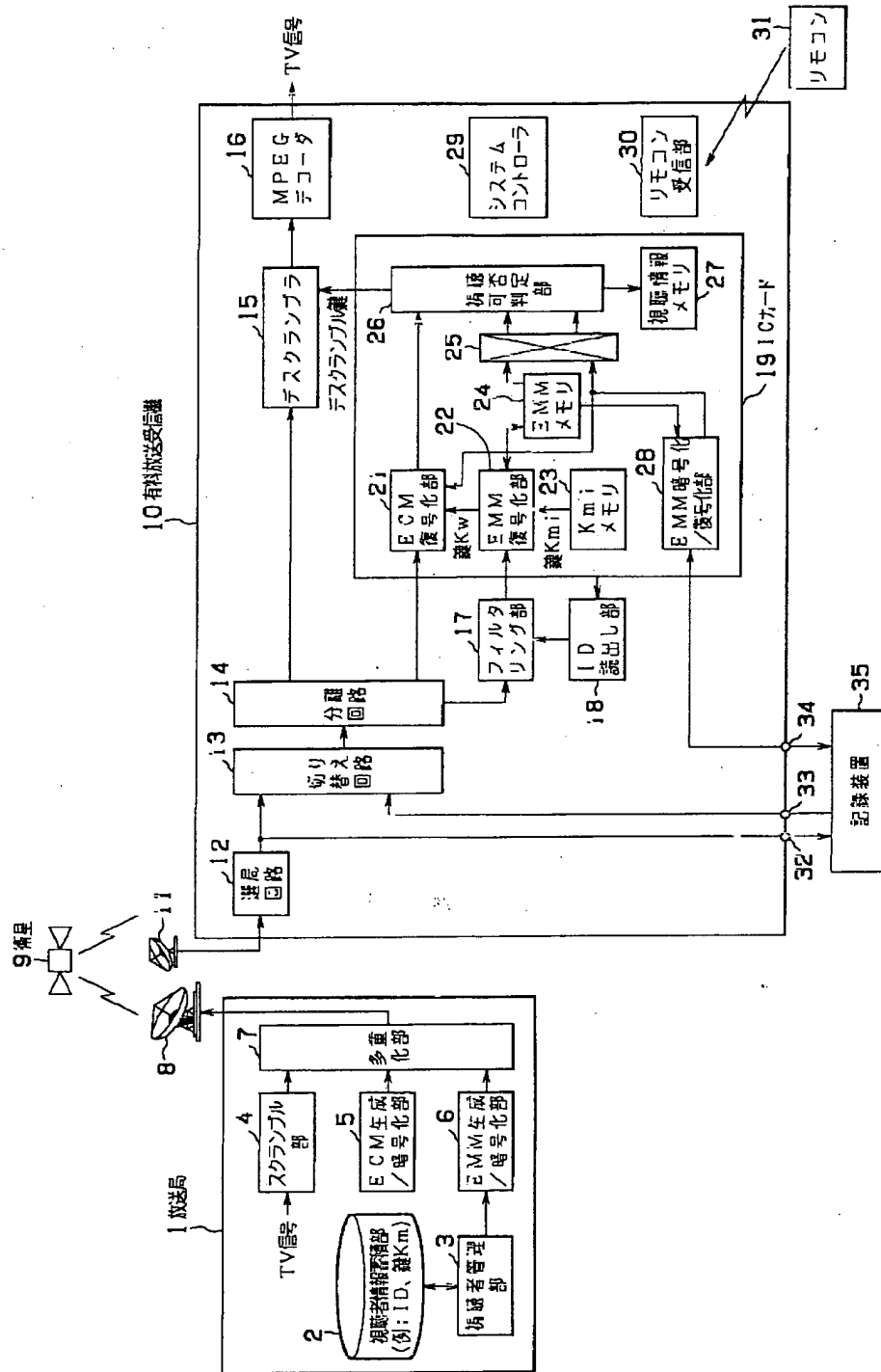
【図3】



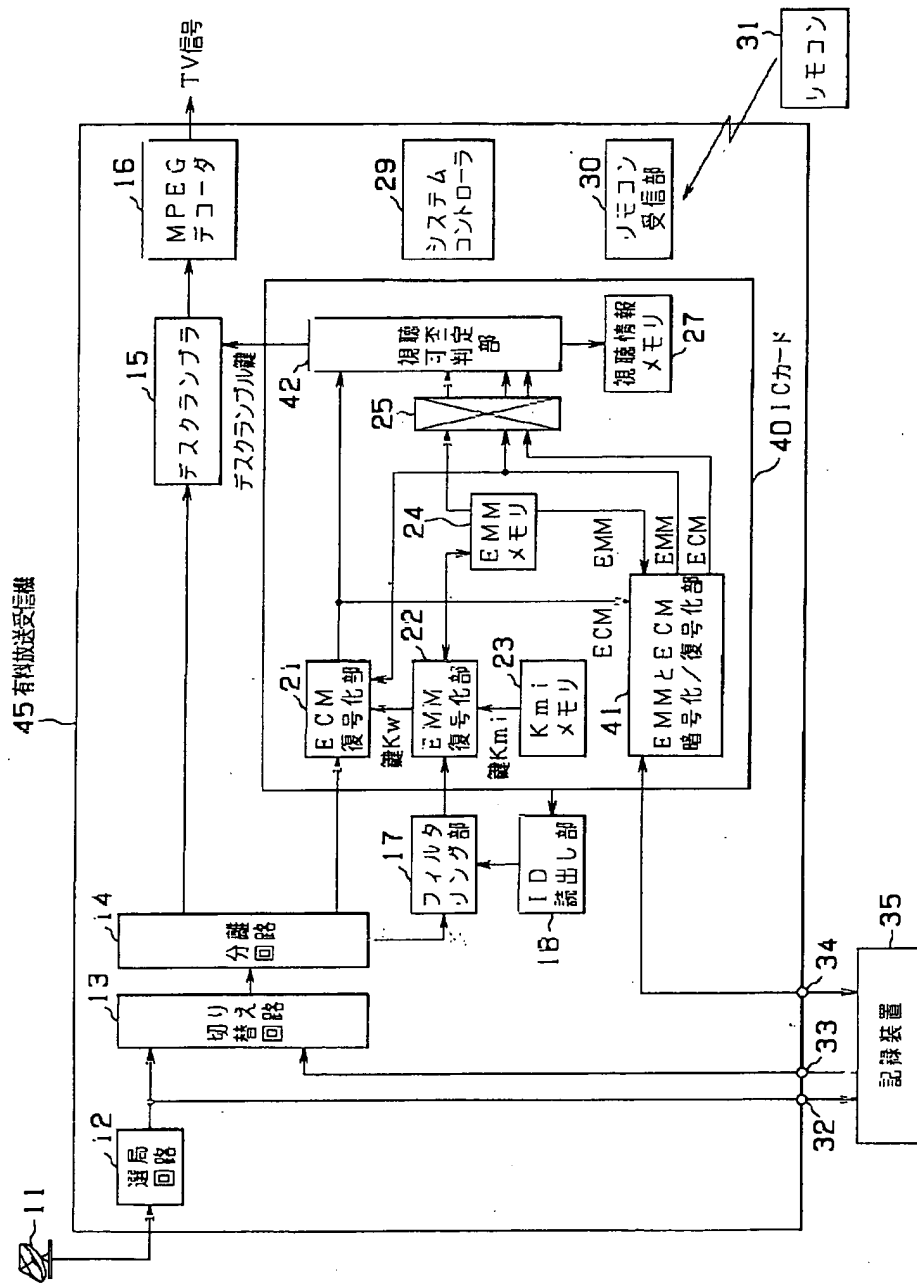
【図4】



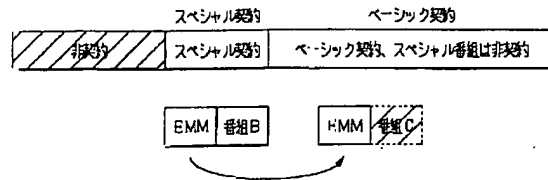
【図1】



【図2】



【図5】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	(参考)		
H 0 4 N	5/44	H 0 4 N	7/167	Z	5 J 1 0 4
	5/76	H 0 4 L	9/00	6 0 1 B	
	5/91			6 2 1 A	
	7/08	H 0 4 N	5/91	P	
	7/081		7/08	Z	
// H 0 4 N	7/20				
	6 3 0				

Fターム(参考) 5C025 AA23 AA30 BA25 BA27 BA30
 DA01 DA04 DA05
 5C052 AA01 DD04
 5C053 FA20 FA21 FA23 HA40 JA30
 LA07
 5C063 AB03 AB07 AC10 CA40
 5C064 CA18 CB01 CC01 DA01
 5J104 AA01 AA16 BA03 EA01 EA07
 EA17 NA03 NA35 NA37 PA04
 PA05